State Privacy Office
April Privacy Tip

9 Ways to Stay Safe Online During Tax Season

It's important to always follow precautionary steps when filing taxes online because you're dealing with sensitive files and information. If this sensitive information were to get exposed, it could put you at risk of identity theft. Here are a few ways you can keep yourself safe during tax season.

1. Update your software

Regularly updating your software is something you should always do. Software updates not only patch security flaws that cybercriminals can take advantage of, but also add new features and improve existing ones.

You should pay particularly close attention to updates for protective software. Be sure your malware and firewall protection is up-to-date before conducting any online transactions. If you don't already have protective software, consider adding it to your device before you begin opening sensitive documents or connecting to a tax-preparation service.

Protective software such as antivirus software will protect your device from having malware installed. When malware is successfully installed on your computer, a cybercriminal can gain access to anything on your machine, placing all your sensitive information and credentials at risk of becoming compromised.

2. Use strong, unique passwords when filing online

This is no time to safeguard your account with passwords like "123456" or reuse passwords across multiple accounts. If you reuse passwords on multiple accounts and one of those accounts is compromised, all of the other accounts are immediately at risk.

Create a password that is at least 16 characters long and includes upper and lower-case letters, numbers and symbols. To create a strong password, use a random password generator. Most password managers like Keeper will generate secure passwords for you and store them safely so you don't have to remember them all yourself. With a password manager, the only password you'll have to remember is your master password, which acts as the key to enter your vault.

3. Enable 2FA wherever possible

If your tax-preparation site offers Two-Factor Authentication (2FA), use it. 2FA is an additional step to your username and password that verifies your identity using an authentication method such as email or text codes, biometric authentication, authenticator apps or physical security keys.

With 2FA enabled, an extra layer of security is added to your account, making it harder for a cybercriminal to compromise it.

4. Back up everything

Ransomware is a type of malware that encrypts all data on your hard drive and demands a ransom payment to unscramble it. The only effective defense is to have a backup, so make sure all of your sensitive financial documents are stored in at least one other place, such as an encrypted cloud service or on a USB drive.

One of Keeper Password Manager's popular add-on services is Secure File Storage. This add-on allows you to store your sensitive documents, files, images and more in your Keeper Vault. No one but you will have access to anything stored in your vault because Keeper's zero-knowledge encryption architecture ensures that only you can access and decrypt your stored files.

5. Don't forget physical security

If your office is in a shared space, your security is only as good as the locks on the door. Store physical records in a safe or file cabinet with a good-quality lock and don't keep old tax records. The statute of limitations on back taxes is three years, although it may be as long as 10 years in some circumstances. Whatever the case, there's no reason to keep those 2005 files around anymore. Shred them.

When possible, store your sensitive physical documents online in an encrypted vault. Not only does this protect your files from getting into the wrong hands, but it also keeps your files safe in the event of a fire, flood or other natural disaster.

6. Don't use public WiFi when filing your taxes online

Public WiFi is never a safe option when accessing the internet. Since the majority of public WiFi networks are unencrypted, anyone can intercept the network and harvest information that is transmitted over it. With something as sensitive as filing your taxes, it's best to do it from a secured WiFi network.

7. Share documents securely with your accountant

Even if your accountant is your best friend, there's no guarantee that person won't get breached. If you need to share documents, upload and store them in a secure password

manager with sharing capabilities. With Keeper's One-Time Share you can securely share records with anyone on a time-limited basis without them having to be a Keeper user.

8. Don't fall for phishing or vishing scams

Scammers love tax season because they know consumers are in a state of high anxiety about the potential of audits or fines. Phishing messages often contain alarming language or threats that are intended to scare recipients into giving up personal information. Any email that appears to be from the IRS and that asks you for personal information is a scam. The basic rules of phishing prevention also apply: don't click on links in an email unless you're absolutely sure of the identity of the sender.

Vishing is also common during tax season. Vishing is a form of phishing that takes place through a phone call. It's important to remember that the IRS never calls taxpayers by phone to request personal information, tax information, credit card numbers or money. If you get a phone call from an IRS impostor, tell them nothing and immediately hang up the phone. Make sure to also report the incident to the Treasury Inspector General at www.tigta.gov.

9. Monitor your filing for suspicious activity

When you file your taxes, the IRS provides you with an Electronic Filing Identification Number (EFIN). You can use this number to check periodically on how many tax returns have been filed in your name. This enables you to catch a breach quickly. After filing your taxes, it's always important to continue to keep an eye open for suspicious activity and your EFIN gives you the ability to do so.

Note: *Your agency/bureau/department/division may have specific requirements – always check your policies and procedures. If you have questions, contact your Privacy Officer.*